REMARKS

Claims 15-21, 23-24, 27-34, and 36-37 are pending in the present application. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Claims 27 and 28 were objected to for a minor error. This has been corrected. Withdrawal of the objection is respectfully requested.

Claims 15-19, 23-24, 27-34, 36 and 37 were rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite. Applicant has amended the claims to address the Examiner's concerns, and overcome this rejection. Applicant respectfully submits that the claims are now fully in compliance with 35 U.S.C. §112. Withdrawal thereof is respectfully requested.

Claims 15-19, 22-24, 27-34, 36 and 37 were rejected under 35 U.S.C. §103(a) as unpatentable over Applicant's admitted prior art in view of Chow (U.S. Patent No. 6,594,761) and Kocher (U.S. Patent No. 6,278,783). Applicant respectfully traverses this rejection.

Applicant's Admitted Prior Art

Applicant notes that, when summarizing the "applicant admitted prior art" as defined in page 2, the Examiner misstates the nature of the prior art. In particular, the prior art always applies the "same" chain of operations in both the server entity and in the card entity (this portion of page 2 refers to "the" DES in the server and in the card).

U.S. Patent No. 6,594,761 To Chow

In Applicant's previous response, herein incorporated by reference, Applicant explained that Chow deals with devising a manner of preventing third parties from obtaining and running unauthorized or unlicensed software (col 1, lines 18-26). Chow defines "tampering" as changing computer software in a manner that is against the wishes of the original author (see lines 57-67 of column 1); this applies when the third party has access to the instructions of the computer software under consideration. This is confirmed in lines 46-54 of column 3 where it is stated the method and system of the invention recognizes that attackers cannot be prevented from making copies and making arbitrary changes.

The solution taught by Chow is a means for receding software code in such a manner that it is fragile to tampering. Attempts to modify the software code will therefore cause it to become inoperable in terms of its original function (col 5, lines 7-10); it is desirable for the program to continue running so that, by the time the attacker realizes something is wrong, the modifications and events which caused the functionality to become nonsensical are far in the past (col 5, lines 15-19). As shown in figure 2, the solution of Chow is applied to a source code so as to provide a tamper-resistant object code (see figure 3 too). Figure 4 deals with an SSA code which is modified into a tamper-resistant SSA code by null coding (see from line 16 of column 13); Figure 5 deals with a SSA code which is modified into a tamper-resistant SSA code by polynomial coding (see from line 56 of column 14); Figure 6 deals with a SSA code which is modified into a tamper-resistant SSA code by residue number encoding (see from top of column 18); Figure 7 deals with a SSA code which is modified into a tamper-resistant SSA code by bit-exploded encoding (see from line 22 of column 19); Figure 8 deals with a SSA code which is modified into a tamper-resistant SSA code by custom base encoding; Figures 9a and 9b deal with a source code which is modified into a tamper-resistant object code by a preferred implementation.

In all cases, the method of Chow results in a tamper-resistant code which is made available to third parties with the intended resistance when such third parties try to tamper the code. Whereas the description mentions some possible choices when implementing the different encoding methods, the modification does not add any selection step to the steps defined in the source code; a code when modified according to the Chow teachings operates in one and a same manner.

U.S. Patent No. 6,278,783 To Kocher

In Applicant's previous response, Applicant explained Kocher deals with DES and other cryptographic processes with leak minimization for smartcards and other cryptosystems (see title). According to the abstract, Kocher discloses methods and apparatuses for improving DES and other cryptographic protocols against external monitoring attacks by reducing the amount (and signal-to-noise ratio) of useful information leaked during processing; there are 2 56-bits keys and 2 64-bits plaintext messages each associated with a permutation such that some equations are satisfied; during operation of the device, the tables are preferably periodically updated, by introducing fresh entropy into the tables faster than information leaks out. According to the sentence bridging columns 1 and 2, secrets (such as keys and/or messages) are divided into separate portions which are then separately mutated, while maintaining mathematical relationships between or among the portions that are used for performing secure cryptographic operations. It is then mentioned that the method provides for improved implementation of the DES as well as other cryptographic operations (col 2, lines 10-13).

In connection with Figure 1 (from bottom of column 8), a message and a key are respectively split in two message and in two keys; the permutations applied to both parts M1 and M2 of a message M (respectively both parts K1 and K2 of a key K) are linked by a relation and the inverse permutations are identified (see, for example, lines 39 to 53 of column 6 or lines 1 to 14 of column 9; these portions state similar comments for M and K). The permuted keys and messages are then used, rather than the standard key and message, during the course of cryptographic operations (lines 53-55 of column 6). Kocher mentions (bottom of column 6) that at the end of the operations, the two parts of the ciphertext may be recombined to form the same encrypted/decrypted quantity that would have been produced by a standard DES protocol.

It thus appears that Kocher teaches to use several keys K1 and K2 (instead of a single one K) and several messages M1 and M2 (instead of a single one M), these keys being derived in a random manner from the normal key and these messages being derived in a random manner from the normal message, it being noted that when one of the messages M1 is randomly determined, the other message M2 is determined from this first determined message, and that when one of the keys K1 is randomly determined, the other key K2 is determined from this first determined key, and it being further being noted that it is necessary to keep trace of the manner the keys K1 and K2, respectively the messages M1 and M2, are derived from K, respectively M, so that inverses can be identified and used when appropriate.

Applicant's Claim 34 (Embodied In Figure 1)

As amended, claim 34 makes it clear that the method includes some steps which are effected once, and other steps which are cyclically effected when appropriate. More precisely, the storing of a first chain of operations (which implement the DES algorithm), together with a corresponding key, in both a server entity and a microcircuit card, as well as the storing of a second set of instructions in the microcircuit card (made of operations which are complements to corresponding operations of the first chain), are steps which are effected as a preparation for a succession of cycles each including the other steps, *i.e.*, the sending of a request from the server to the card, the sending of a message from the card to the server, the executing of said first chain of operations on this message in the server and the executing of either the first chain of operations or the second chain of operations (with an additional complementation instruction), the comparing of the resultant message at the card entity with the result message at the server entity and the validating the cryptographic protocol when the result message and the resultant message are identical.

Thus, this method involves two entities using one and a same key; a given message (generated by the card entity when it receives a request from the server entity) is submitted in parallel to a treatment in the server (*i.e.*, the DES) and in the card (either the same DES or the DES as complemented (further including a complementation instruction), and a comparison is made between the results of the parallel.

The difference between the first and second chains of operations which are stored in the card entity only differ by a complementation applied to each operation (and an additional complementation); in other words, the difference between the parallel treatments, when it exists, is rather simple. On the other hand, the invention is, in particular, based on the fact that the inventors realized that it was possible to submit a message to either a DES or a "complemented DES" while obtaining a same result so that successive validations of a protocol remain possible without always applying the same DES to a message in the card entity. This is a key difference with respect to the admitted prior art where the parallel treatments were always the same, in the server entity as well as in the card entity. Applicant submits that neither Chow nor Kocher would have led the person ordinarily skilled in the art to think that a validation could be made with different treatments in the server and the card, respectively.

The Comments Of The Examiner About Chow And The Combination Of Its Teachings With The Invention Of Claim 34

The Examiner asserts that Chow discloses a tamper-proof encoding method that can be used with an encryption protocol and refers to the description from line 28 of column 20. This part explains that one may hide Data Encryption Standard (DES) keys using Bit-Exploded (see from line 31 of column 18) and Bit-Tabulated coding (from line 43 of column 19); it further explains that application of such encoding on a routine with an embedded key results in a tamper-resistant software routine which still performs DES encryption, but for which extraction of the key is a very difficult task (lines 36-41). Applicant thus considers that even this part of the description teaches to modify a source code into a tamper-resistant object code which operates in one and a same manner.

The Examiner asserts that Chow discloses that the encoding method includes determining whether to perform an operation or its complement; he refers to the description portion from line 50 of column 18 to line 13 of column 19. In fact, in Applicant's understanding, this part only states that, when the tamper-resistant code has been encoded, any determination has been made and no choice remains when such code is operated.

Then the Examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state in order to increase the tamper-resistance and obscurity of computer code. For the reason explained in the preceding paragraph, Applicant respectfully disagrees with the Examiner as to the extent of the teachings of Chow.

In fact, Applicant submits that Chow would have only led a person ordinarily skilled in the art to improve (by making it tamper-resistant) the DES which is used in the admitted prior art, *i.e.*, the DES used in both the server and in the card. In other words, the admitted prior art when modified according to the teachings of Chow would apply identical DES in the server and in the card, the difference with respect to the admitted prior art being that the DES has been made tamper-resistant (see the definition of "tampering" at the bottom of column 1 of Chow).

Applicant submits that, when reading Chow, the person ordinarily skilled in the art would not have been led to admit, to modify the admitted prior art, so as to have different treatments in the server and in the card. In any case, this person skilled in the art would not have been led to have, in the card, different treatment which a random selection is made in the successive cycles of validation.

Thus, Applicant submits that the method of the admitted prior art when modified according to Chow would differ from the invention of Applicant's pending claim 34 by the fact that, in the successive cycles of validation, a message exchanged between the server and the card is submitted in parallel to treatments which are sometimes different, sometimes identical, the selection of the cycles where the treatments are identical and the cycles where the treatments are different being made randomly. Applicant thus submits that the differences between the invention and the admitted prior art as modified by Chow are far more significant than the single difference mentioned in the paragraph bridging on pages 10 and 11 of the Office Action.

Comparison Made By The Examiner Between Applicant's Invention Of Claim 34 And The Admitted Prior Art Modified In View Of Chow And By Kocher

The Examiner asserts that it would have been obvious to one of ordinary skill in the art to modify the method of the admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of the system.

Applicant already explained that the admitted prior art as modified by Chow does not only differ from the invention by the existence of some random determination. In any case, since Kocher teaches to modify a cryptographic process involving a DES so as to split a message to be submitted to operations as well as the key to be used during such operation, Applicant submits that the admitted prior art as modified by Chow as further modified according to the teachings of Kocher would have led the person ordinarily skilled in the art to splitting of the message and of the key before applying the parallel treatments in the server and in the card, respectively.

This modification would not have led the person ordinarily skilled in the art to a method where, in the successive cycles of validation, a message exchanged between the server and the card is submitted in parallel to treatments which are sometimes different, sometimes identical, the selection of the cycles where the treatments are identical and the cycles where the treatments are different being made randomly.

Applicant thus submits that the invention of pending claim 34 is patentable over the cited prior art.

In addition, Applicant submits that the above admitted prior art method as modified by Chow and then by Kocher fails to teach or suggest to modify, in some cycles, the step of randomly selecting which group to apply to the message depending on a difference between the number of cycles where the group applied to the message was the first chain of operation and the number of cycles where the group applied to the message was the complemented chain of operations. The Examiner asserts that this is anticipated by the fact that Kocher discloses comparing a counter against a threshold value and altering operation based on the comparison (col 9, lines 25-30 and col 7, lines 21-29); but it has already been explained that such comments of Kocher deal with the treatments of both parts of a key and a message and do not deal with the DES in its whole.

Applicant thus submits that the subject-matter of claim 24 is patentable too over the cited prior art.

Other claims depending on claim 34 are patentable since claim 34 is patentable.

About The Invention Of Claim 36 (Embodied In Figure 2)

As amended, claim 36 makes it clear that the method includes some steps which are effected once, and other steps which are cyclically effected when appropriate. More precisely, the storing of a first chain of operations (DES), together with a corresponding key, in both a server entity and a microcircuit card, as well as the storing of a second set of instruction in the microcircuit card (made of operations which are complements to corresponding operations of the first chain), are steps which are effected as a preparation for a succession of cycles each including the other steps, *i.e.*, the sending of a request from the server to the card, the sending of a message from the card to the server, the executing of said first chain of operations on this message in the server, the identifying and selecting of a selected chain of operations and the executing of this selected chain of operations, the comparing of the resultant message at the card entity with the result message at the server entity and the validating the cryptographic protocol when the result message and the resultant message are identical.

Thus, this method involves two entities using one and the same key; a given message (generated by the card entity when it receives a request from the server entity) is submitted in parallel to a treatment in the server (*i.e.*, the DES) and in the card (a selected chain of operations identical to this DES or differing from this DES by at least one operation being complemented, and a comparison is made between the results of the parallel treatments.

Applicant notes that the difference between the DES applied in the server and the selected chain of operations applied to a message in a given cycle, when there is a difference, only deals with complementation of at least some of the operations of the DES; in other words, the difference between the parallel treatments, when it exists, is rather simple.

On the other hand, the invention is, in particular, based on the fact that the inventors realized that it was possible to submit a message to either a DES or a chain of operations only differing from the DES by complementation of at least some of the operations while obtaining the same result so that successive validations of a protocol remain possible without always applying the same DES to a message in the card entity. This is a key difference with respect to the admitted prior art where the parallel treatments were always the same, in the server entity as well as in the card entity. Applicant submits that neither Chow nor Kocher would have led the person ordinarily skilled in the art to think that a validation could be made with different treatments in the server and the card, respectively.

Chow And The Combination Of Its Teachings With The Invention Of Claim 36

The Examiner asserts that Chow discloses a tamper-proof encoding method that can be used with an encryption protocol and refers to the description from line 28 of column 20. This part explains that one may hide Data Encryption Standard (DES) keys using Bit-Exploded (see from line 31 of column 18) and Bit-Tabulated coding (from line 43 of column 19). It further explains that application of such encoding on a routine with an embedded key results in a tamper-resistant software routine which still performs DES encryption, but for which extraction of the key is a very difficult task (lines 36-41). Applicant thus considers that even this part of the description teaches to modify a source code into a tamper-resistant object code which operates in one and the same manner.

The Examiner asserts that Chow discloses that the encoding method includes determining whether to perform an operation or its complement; he refers to the description portion from line 50 of column 18 to line 13 of column 19. In fact, in Applicant's understanding, this part only states that, when the tamper-resistant code has been encoded, any determination has been made and no choice remains when such code is operated.

Then, the Examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state in order to increase the tamper-resistance and obscurity of computer code. For the reason explained in the preceding paragraph, Applicant disagrees with the Examiner as the extent of the teachings of Chow.

In fact, Applicant submits that Chow would have only led a person skilled in the art to improve (by making it tamper-resistant) the DES which is used in the admitted prior art, *i.e.*, the DES used in both the server and in the card. In other words, the admitted prior art when modified according to the teachings of Chow would apply identical DES in the server and in the card, the difference with respect to the admitted prior art being that the DES has been made tamper-resistant (see the definition of "tampering" at the bottom of column 1 of Chow).

Applicant submits that, when reading Chow, the person ordinarily skilled in the art would not have been led to admit, to modify the admitted prior art, so as to have different treatments in the server and in the card. In any case, this person ordinarily skilled in the art would not have been led to have, in the card, different treatment which a random selection is made in the successive cycles of validation.

Thus, Applicant submits that the method of the admitted prior art when modified according to Chow would differ from the invention of Applicant's pending claim 34 by the fact that, in the successive cycles of validation, a message exchanged between the server and the card is submitted in parallel to treatments which are often different, but sometimes identical, the selection of the cycles where the treatments are identical and the cycles where the treatments are different being made randomly. Applicant thus submits that the differences between the invention and the admitted prior art as modified by Chow are far more significant than the single difference mentioned in the paragraph bridging on pages 10 and 11 of the Office Action.

The Comparison Made By The Examiner Between Applicant's Invention Of Claim 34 And The Admitted Prior Art Modified In View Of Chow And By Kocher

The Examiner states that it would have been obvious to one of ordinary skill in the art to modify the method of the admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of the system. Applicant already explained that the admitted prior art as modified by Chow does not only differ from the invention by the existence of some random determination. In any case, since Kocher teaches to modify a cryptographic process involving a DES so as to split a message to be submitted to operations as well as the key to be used during such operations, Applicant submits that the admitted prior art as modified by Chow as further modified according to the teachings of Kocher would have led the person ordinarily skilled in the art to splitting of the message and of the key before applying the parallel treatments in the server and in the card, respectively.

This modification would not have led the person ordinarily skilled in the art to a method where, in the successive cycles of validation, a message exchanged between the server and the card is submitted in parallel to treatments which are sometimes different, sometimes identical, the selection of the cycles where the treatments are identical and the cycles where the treatments are different being made randomly.

Applicant thus submits that the invention of pending claim 36 is patentable over the cited prior art.

In addition, Applicant submits that the above admitted prior art method as modified by Chow and then by Kocher fails to teach or suggest to modify, in some cycles, the step of randomly selecting the selection of operations depending on a difference between the number of operations which have been selected in the chain of noncomplemented operations and the number of operations which have been selected in the chain of complemented operations.

Applicant thus submits that the subject-matter of claim 33 is patentable over the cited prior art.

For at least these reasons, Applicant respectfully submits that claims 34 and 36 are patentable over the cited prior art, alone or in combination as proposed in the Office Action. Claims 15-21, 23-24, and 27-33 are believed to be patentable in and of themselves, and for the reasons discussed above with respect to claims 34 and 36.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:srd
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\R\RINU\Akkar1\pto\2013-05-02Amendment.doc